Ovum
TMT intelligence | informa

Effective Vulnerability Risk Management

Maintaining security and compliance in a modern IT supply chain

Publication Date: August 14, 2018

Author: Roy Illsley

Summary

Catalyst

The reality for many data center managers is that the walls are now flexible and extend from the on-premises environment to the cloud. This brings with it new challenges and threats. The biggest threat is that the surface area for attackers has significantly increased, and with this increase comes an equal increase in complexity, which all translates to greater risk. For data center managers, the need to ensure that systems remain compliant is not therefore enough, because the compliance policies are a reaction to an existing threat. Ovum believes that new approaches are required to ensure that an organization's environment is secure and compliant, and new tools and software are needed to deliver this.

Key messages

- The security and risk management of an organization's environment is now a complex mixture of known and unknown threats and actors.
- Current solutions do not fully support the DevOps lifecycle approach to application development and management.
- Extending automation beyond the data center requires a new approach and thinking about management.
- Dealing with the new security threats will put pressure on the current approach to regulatory compliance and patch management.

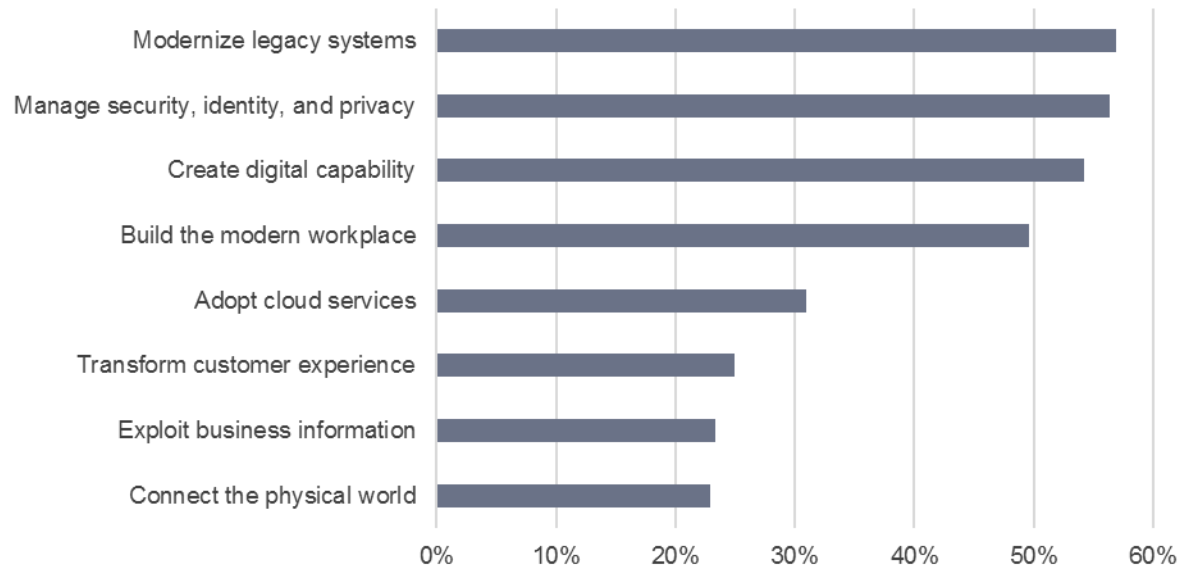
Recommendations

Ovum believes that providing comprehensive vulnerability and risk management in a complex modern IT supply chain that consists of multiple public clouds and a range of technologies from VMs to containers represents a significant business benefit. To mitigate the risks that organizations are facing from the increasing surface area being presented to the attackers requires them to ensure orchestration and automation are used in tandem to deliver an integrated approach. This is needed because only being compliant does not translate to also being risk-free. The two elements must be considered side by side to provide improved security.

Market context

The security of an organization's environment is now a complex mixture of known and unknown threats

Figure 1: Security and modernization are the top two targets for 2018/19 IT spending



Source: Ovum ICT Enterprise Insights 2017/18 n=4,798

Figure 1 shows the intended IT spending priorities for 2018/19 from Ovum's annual global *ICT Enterprise Insights* survey, n=4,798. The survey discovered that over 56% of respondents place security as a top three spending priority in 2018/19. The top priority is modernization of legacy systems, which also has security implications. When this intended spending is looked at through the eyes of a chief security officer (CSO), its significance becomes more apparent. The environment that CSOs must protect is increasingly becoming more complex, with about 30% of workloads currently being delivered from the cloud. The other contributor is that organizations are adopting a multicloud strategy that includes two or more public cloud providers as well as a hybrid on-premises cloud.

This complexity creates an increased surface area where threats or threat actors can attack. Ovum's market forecast data shows the vulnerability and risk management market growing at a CAGR of over 10% by 2022, with some geographies growing at over 16%. This is the third fastest growing segment of the security market behind DDOS and network security management, and Ovum believes that this focus on vulnerability and risk management is driven by the fact that there are as many unknown threats as there are known threats, and that being able to prioritize and mitigate these as quickly and efficiently as possible is a business imperative. In fact, in Southeast Asia ransomware is the number-one threat, according to Ovum's 2017 cloud storage survey, with over 46% respondents in Japan and Singapore saying it was important or very important. However, it is the unknown threats that represent the future challenge for CSOs, and this means having a strategy for managing risk, with processes to deal with remediation or containment.

Challenges of maintaining more than only compliance

Current solutions do not fully support the DevOps lifecycle approach to application development and management

The rise of the DevOps culture and movement was popular because it transformed the development, delivery, and maintenance of applications to become a continuous delivery process. However, this transformation required new tools and processes to be adopted by all the constituents involved, from developers to operations. Micro Focus with its Data Center Automation (DCA) solution provides an example of how the new tooling operates. DCA has a single UI that performs scans, remediation, and visualization for regulatory compliance risks and vulnerabilities across server OSes, databases, and middleware. DevOps solved one major problem with operating a continuous delivery process, enabling better collaboration and removing the siloed mentality of the waterfall approach to application development and delivery, but it created a new challenge. Configuration management tools such as Puppet, Ansible, and Chef have become widely used by DevOps teams to automate the delivery pipeline, but this has created a blind spot for central IT operations. These configuration management tools automate and report on the configuration status of the infrastructure involved in the application delivery process, but the ability to have a more holistic view is somewhat restricted. Central IT operational teams are typically responsible for a multitude of different environments and must be able to manage configurations, change policies, and manage patch levels based on more than a narrow application-centric view.

One of the issues that organizations must be cognizant of is that data tracked by these configuration management tools can quickly fall out of date and produce erroneous reports. The effect of this is to reduce the tool's value to the enterprise because the information it provides in relation to risk and vulnerability is compromised. Ovum believes that the integration between configuration management tools and the planning process is also an area that must be fully understood. These gaps in configuration management require an overarching capability that can link understanding the granular configuration details to the higher-level risk and vulnerability of the organization.

Extending automation beyond the data center requires a new approach to thinking about management

The greater use of automation is seen as an inevitable next step in the drive to increase IT operational efficiency. Automation is, however, only a means of executing a set of commands or instructions, and on its own it has limited value. Ovum believes that to make automation a valuable business tool requires an orchestration capability to be closely linked with it. Building a continuous compliance capability using automation and orchestration is seen as the most appropriate way to effectively deliver vulnerability and risk management. The market has treated these two capabilities as separate, yet building orchestration into the different solutions and integrating an automation engine seems logical but remains rare.

Another key aspect of extending the role of automation and orchestration is the ability to work across the many different environments that IT must contend with. The growth of acceptance in enterprise customers of open source technologies has seen a significant increase over the past few years. In

fact, open source is a prime driver of the container and microservices architectures that organizations are beginning to adopt at scale. However, maintaining compliance in this diverse ecosystem of technologies requires a solution to be able to understand the different threats they represent. This scenario is further complicated by the expansion of cloud computing, particularly the use of multiple public clouds. When the need to orchestrate and automate the management of policies for databases, middleware, and container-based cluster nodes is overlaid, the challenge becomes more complex. This new reality creates a mesh of interrelated components in different locations based on different technologies, all of which represent risks to be mitigated and managed. The use of standard out-of-the-box templates that provide quick-start guides to provisioning is a useful concept that can ensure that organizations get rapid time to value from any solution. However, these templates, or blueprints, must be provided for a range of different environments and cover difference compliance regulations. DCA, for example, provides benchmarks and remediation actions aligned to the latest industry and regulatory guidance for CIS, PCI DSS, SOX, FISMA, HIPAA, and more.

Dealing with the new security threats will put pressure on the approach to regulatory compliance and patch management

The challenges of dealing with the new reality of multiple systems and emerging technologies requires a new approach to vulnerability and risk management. As the nature of the threats becomes equally diverse, a single platform-based approach is needed. The clear advantage of a platform-based approach is that different modules and capabilities can be added as they are needed. When organizations consider the requirements of any approach to vulnerability patch management, they should not lose sight of the need for regulatory compliance to ensure any remediation is in line with the rules for their industry. Making sure the infrastructure is both secure and compliant presents challenges for discrete tools that only see part of the picture. The scaling of any deployment is also another consideration, and using a containerized platform will enable it to deliver a consistent performance as the environment grows.

The other issue with discrete tools is that as the business expands, the number of threats also increases. A typical response to this is to employ more people to manage the increased threat level. This increase in staffing numbers means that the discrete activities of scanning, reporting, and patching must be increased in line with one another. The result is that this just increases the cost-base and does not usually deliver improved compliance. This scenario is precisely where the automated and orchestrated platform approach becomes operationally effective. Using a single version of the truth that can be presented to the different actors, using a language they are familiar with, can significantly improve decision-making. Ovum believes that having a compliance and risk dashboard represents one approach to presenting the information in an easy to digest way, and tools such as DCA provide this visibility into compliance and patch status across the infrastructure stack. DCA enables users to drill down through the dashboards to show the compliance level by severity, including the efficiency of the remediation process (for example, how long it took to remediate), the latest critical and high-level threats, the resources impacted, and the age of vulnerabilities.

Ovum view

As the IT environment becomes increasingly complex and distributed, the challenges of ensuring security and compliance also increase. Canada's Prime Minister, Justin Trudeau, said at the economic summit in Davos Switzerland in 2018: “The pace of change has never been this fast, yet it will never be this slow again.” This statement demonstrates the need for organizations to adopt new approaches to dealing with technology evolution, and to make sure it is applied securely and according to the governance rules under which the company operates. To achieve this, automation and the use of machine learning will be needed to coordinate all the moving parts of the new reality, and automation must be adopted in a way that fits with an organization's culture. Ovum believes that this means using a flexible solution and applying it in stages at the pace of the organization, not that dictated by the vendor.

Appendix

Author

Roy Illsley, Principal Analyst, Infrastructure Solutions

roy.illsley@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo